American Health Information Community

Confidentiality, Privacy, and Security Workgroup

Comments on Working Hypothesis

June 22, 2007

Lockheed Martin is pleased to respond to the American Health Information Community (AHIC) Confidentiality, Privacy, and Security (CPS) workgroup questions. Lockheed Martin brings an extraordinary breadth of experience in achieving interoperability standards among competing organizations, and in integrating data from an enormous range of standalone systems. As the largest information technology contractor to the federal government, Lockheed Martin has consistently demonstrated the ability to reach beyond broad policy goals into the detailed requirements and business rules required to develop and maintain complex, secure system integration projects. We believe our experience and performance on behalf of civilian agencies of the federal government, for Department of Defense and Veterans Administration clients, and for the intelligence communities gives us important insights into many of the questions the Confidentiality, Privacy, and Security workgroup has posed.

Overview and Summary

Lockheed Martin has a wide and varied base of experience in the areas of confidentiality, privacy, and security protections. In our responses to the questions, we have discussed many of the problems associated with these areas, what issues typically arise, the options to consider, implementation strategies, and ongoing support considerations. There are

several over-arching considerations in the area of confidentiality, privacy, and security protections which will have an affect on the direction, pace, and success of any federated implementation.

The nature of the challenge is one in which mandates and control are not clearly defined or consistently adhered to across the industry. Although various policies, rules, laws, and statutes discuss what is or is not permissible, success within a defined community of providers have a greater chance of success and are greatly increased over those of the larger and more distributes health services connecting through NHIN or RHIOs. The complexities of various vendor provided CPS implementations, data availability, data integrity, data accessibility, middle-ware, authentications, or jurisdictions could all but stymie any progress these initiatives have made.

Lockheed Martin believes there are specific areas of concern, of which we will mention here and include as part of our specific responses to the questions. We recognize the challenges associated with unique identity authentication when linking records including the process and mechanisms for: establishing an understood level of confidence that the identifier refers to a specific individual (individual authentication); the process of establishing an understood level of confidence that an identifier refers to an identity (identity authentication); the process of establishing an understood level of confidence that an attribute applies to a specific individual (attribute authentication); the process to limit who enters or accesses a give system/resource or to control what they have access to

once they are in the system (identity access and control systems); the process for monitoring the system to include audits, accountability, rewards, and support decisions. The processes need to integrate very tightly into the fabric of the environment, ensuring that any breach of security is quickly identified, data integrity and validity are managed, external systems interfaces are managed, oversight and assurance of consumer rights and data control, and the many contractual relationships and legal implications and how markets will or won't support the emerging environment and systems support requirements.

1. Enforceable mechanisms

The workgroup is interested in comments on appropriate, effective, and feasible ways to enforce confidentiality, privacy, and security protections in an electronic health information exchange environment. Technical solutions will continue to evolve. Critical methods for enforcing privacy and security standards include identity management, role-based access controls, and access authorization and authentication. The workgroup should consider guidance or requirements to facilitate development of structures and processes to manage across covered entities, such as policy boards, technical review boards, and strategic planning forums.

The greater challenge in electronic health information exchange is managing growth of a highly complex and heterogeneous healthcare environment. Lockheed Martin recommends that … [insert recommendation here].

In organizations such as those we support within the DoD, where adherence to policy and directives are not voluntary, but mandatory, we see the cycle times shorter and the adoption and compliance rates much higher. This in-turn has helps to manage costs and further enforce the fundamental principles that the CPS working group are charged with today.

a) Lockheed Martin has employed identity management and access control systems such as the SUN Identity Management solution at the Centers for Medicaid and Medicare Services. The solution allows for the management of identity-related objects stored in the Directory Server. This allows for the creation and deletion of specific objects as well as the ability to get, add, modify, or remove the attributes of these objects. With this solution, Lockheed Martin is able to leverage the Local Directory Access Protocol services to manage the configuration information for identity-related objects and a Java Software Development Kit (SDK) to embed the management functions into applications or services. This allows for the overall enhancement of the security services and functionality of the entire environment, for capabilities such as; managing user identities across a variety of applications in order to provide provisioning and secure access, ensuring ongoing compliance and enable federation for sharing beyond a single network boundary. The environments that Lockheed Martin supports are vast and the importance of protecting sensitive enterprise information against

security threats, both internally and externally for our customer, have become more manageable in terms of reducing risk and providing more centralized control for security operations.

b) Lockheed Martin has implemented a Role-based Access Control system, to further strengthen security practices and further leverage Identity Management and Access Control Systems capabilities. A federated industry will need to not only provision accounts and access, but including additional controls over the types of data that can be accessed, modified, updated, or deleted requires the ability to implement the forcing function to mandate data integrity mechanisms work at not only the system or application level, but also extend beyond the perimeter of the local environment.

c) Lockheed Martin has also managed the implementation of Homeland Security Program Directive – 12 (HSPD-12), managing the end-to-end program for several agencies. Many of our military and healthcare customers are now required to implement HSPD-12, integrating it into the fabric of their infrastructure and environments. This capability, coupled with security measures like those mentioned above, provide a well rounded approach to ensuring only authorized access to data is granted to those who need it.

2. Relevant requirements

The workgroup requests comment as to whether particular confidentiality, privacy, and security requirements equivalent to those in the HIPAA Privacy and Security Rules should or should not apply to a particular type of person or entity and why.

Lockheed Martin's assessment of HIPAA Privacy and Security Rules, is that although a lot has been done to address many issues, we believe the movement away from specific technology implementations and more toward security management principles and broad management controls for protecting patient health information has only weakened the ability to implement and manage a strong environment of confidentiality, privacy, and security. Although security and privacy are inextricably linked, a lack of structure and strong oversight may make any implementation over-burdensome and unmanageable. As communities become more reliant, what becomes more important is ensuring the integrity and availability of data. Most RHIOs have acknowledged that back up and availability are lacking, further underlining the focus on these items. These Privacy and Security Rules will have a profound impact on things such as Disaster Recover and the nation's approach to pandemic planning. Initiatives such as the National Provider Identifier are the underpinnings of privacy and security to foster appropriate authorization and access.

Lockheed Martin believes exempting participants in local or national health information exchange initiatives from HIPAA requirements would create more problems than it solves. Lockheed Martin also believes some HIPAA provisions should be enhanced, due to the following concerns:

a) The scope of the final Security Rule was limited to all electronic health information pertaining to individuals. The Rule also addresses "protected health information" (PHI), but limits its scope to only PHI that is in electronic form. This is where HIPAA Privacy Rule (164.530(c)) still requires the appropriate measure of security for all PHI, regardless of its format. This is particularly challenging when the context of the discussion is around NHIN, RHIOs, Hospitals, Clinics, Physicians offices and the many vendors who provide the needed support. The management and oversight of these systems are a daunting task and governance is a particular challenge.

b) On a positive note, the final Security Rule established definitions for many of the terms used in HIPAA, helping to eliminate inconsistencies. Several terms were removed from various sections of HIPAA (164.501 and 164.504) and placed in section 164.103, and also apply to the Security Rules, including the terms Plan Sponsor, Protected Health Information, Common Control, Common Ownership, Health Care Component, and Hybrid Entity. These changes greatly enhance the context of focus areas for the CPS workgroup, but as we stated above, governance across the industry will remain a challenge.

c) Lockheed Martin also recognizes the move away from highly prescriptive security requirements. With the pace of technology changes, political drivers, and public health demands, it is obvious that the approach of having a more broad based set of standards that define in generic terms what is needed, should allow for a more

scalable, flexible and generally addressable set of security practices through various approaches and technologies. Although Lockheed Martin agrees in principle, we also recognize, through our membership in a number of standards bodies and enterprise implementations, the many challenges that face the community in achieving the right balance between confidentiality, privacy, security, and the ability to tie it all together.

d) HIPAA was intentionally designed to allow for a certain degree of flexibility because of the differing size and capacity of covered entities. We are not suggesting that this was a bad idea simply that the impacts on covered and non-covered entities will be difficult to manage. Implementation specifications are another area where direction has become broadened to move away from specific implementations to an approach that describes the actions that should be taken to ensure compliance. We find it interesting that only 13 of these implementation specifications are required and the remainder are "addressable." This leaves a lot to the discretion of the organization that is implementing and offers the opportunity to opt out of some of the more fundamental specifications. This further breaks down the "glue" that holds the security picture in place.

e) The General Rules provision of the security standards section 164.306 require covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains, or transmits; protect against any reasonably anticipated

threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and ensure compliance by its workforce. Although these General Rules specify that covered entities comply with the standards for Administrative Safeguards, Physical Safeguards, Technical Safeguards, Business Associate Contracts, and Policies, Procedures, and Documentation, they still afford covered entities three options: implement the specification, implement an alternative security measure to accomplish the purposes of the standard, or not implement anything if the specification is not reasonable and appropriate AND the standard can still be met.

3. Business Associates

The workgroup is seeking comments on the pros and cons of having business associates directly responsible for HIPAA requirements – though not through contractual arrangements. Specifically, the workgroup would like business associates to answer the following questions:

A) How does your organization ensure compliance with the privacy and security policies of covered entities with whom it contracts, particularly when there are numerous contracts?

Lockheed Martin's approach to ensure compliance with privacy and security policies within the customer communities we support, such as the Centers for Medicare & Medicaid Services, is to develop a strong partnership based on a

fundamental understanding that Lockheed Martin adopts the customer's privacy and security policies, integrating the necessary practices into our business model and processes to ensure alignment and congruency in purpose and practice. Lockheed Martin leverages the knowledge and experience of being the nation's leading systems integrator, to facilitate the compliance of interfaces between multiple agencies and contracts. A lot of this capability is further enhanced by the implementation of various boards, working groups, and integrated product teams. This enables the ability to work together to evaluate guidance, implement change, and manage configurations, ensuring compliance with a wide array of policies, guidelines, and rules.

B) How do you handle business associate contracts with large numbers of covered entities including compliance with each covered entity's privacy policies?

Each contract Lockheed Martin engages in has some level of compliance for privacy policies. These policies are managed by incorporating specific policies for Lockheed Martin personnel, reinforcing that through periodic training. We also incorporate those privacy policies in the way we do business; the SUN Identity Manager listed above is but one example of how we implemented HHS security and privacy policies for the Centers for Medicare & Medicaid Services. Through the use of things like the Local Directory Access Protocol, technical security and privacy policies can be implemented on a local as well as enterprise level.

C) How are business associate agreements negotiated? Do you have a standard contract?

Lockheed Martin has several mechanisms and approaches for business associate agreements. They can range from a simple Service Level Agreement between functional organizations, to Service Level Agreements between Contracts, to Terms of Reference Plans between Industries and agencies. These are typically developed locally and then worked through partnerships or membership in an integrated product team. In the context of HIPAA and Security Rules, they provide the over-arching guidance for business services, and local business associates have the latitude to strengthen the policies and guidelines at the system interface leading back into their environments. But, all must agree on the lowest common denominator at the enterprise level and be able to demonstrate compliance. The appendix lists a number of programs where Lockheed Martin has implemented this model, both at a business and operational level.

D) How is the data protection compliance of subcontractors ensured and/or assessed?

Lockheed Martin approaches this topic from a "Defense in Depth" perspective. We are well versed in the area of data protection, as the nation's number one defense contractor, this is part of the way we do business. Data protection compliance spans the entire environment, from the human and physical connection, to the network connection, to the host connection, to the application, to the data itself. We implement various provisioning processes, identity management and access control, authentication mechanisms. We

leverage logical isolation approaches. We use Remote Access Services and Virtual Private Networks. We leverage firewalls, intrusion detection systems, intranet, and extranet solutions. We also have implementations of Role-Based Access Control, when individuals are only authorized to see certain data, based on their particular function. To ensure compliancy, we conduct training and various audits, from our processes and procedures, to the actual operational environment, validating that we say what we are doing, and doing what we say.

E) Do you have subcontractors and how do you handle those agreements?

Lockheed Martin has hundreds of contracting companies and thousands of individual contractors that support our various programs across many environments. When dealing with the federal government, we leverage the "flow-downs" within the Federal Acquisition Regulation (FAR) pertaining to subcontractors, ensuring that they agree and signup to the same rules and regulations that the prime contractor agrees to. When dealing with agencies that are not bound by the FAR, Lockheed Martin includes language in our "Terms & Conditions" that ensure our subcontractors are bound by the same requirements as Lockheed Martin. This contractual language is specified and agreed to before any work commences with the contracting agency. As such, all subcontractors are bound by the same contractual language that Lockheed Martin signs up to with the particular customer. Further, training is conducted with each new hire (Lockheed Martin or subcontractor) to familiarize them with the operating agreements for each engagement. Lockheed Martin has a

strong governance program that includes policy and procedure reviews, as well as audits to ensure that we are following those processes and procedures, which both Lockheed Martin employees and subcontractors are subject to.

F) How would direct accountability for meeting relevant HIPAA requirements impact your business?

Meeting relevant HIPAA requirements has a more profound impact on the customers we serve. It affects their budgets and operating models, ensuring that they have the right balance between compliance and performance. Direct accountability for meeting relevant HIPAA requirements for Lockheed Martin would have varying degrees of impact. The 13 required Security implementation specifications and the privacy requirements lean toward providing the high-level guidelines for an enterprise to function, but leave out enough specificity that it requires a lot of intermediate work to be negotiated and performed. Lockheed Martin has implemented many forms of the requirements associated with confidentiality, privacy, and security, and have adopted similar guidance as part of the way Lockheed Martin does business internally. Because we understand the value that can be attained though such guidance, we would encourage the CPS working group to push for a stronger voice in implementing policies and guidance as they pertain to confidentiality, privacy, and security.

4. General Questions

The CPS workgroup is seeking comment on any of the following additional questions.

A) What are the implications of having some entities performing similar services covered by federal law (e.g., HIPAA) and others not? For example, a personal health record (PHR) could be offered by a health plan (covered entity) and an independent PHR service provider (non-covered entity).

i. How does this impact your competitiveness?

ii. How does this impact your ability to exchange information with others?

iii. Does contracting with non-covered entities create different levels of accountability and/or enforceability in the exchange of health information?

There are obvious differences in terms of compliance between covered and non-covered entities. The issues are wide and varied. This question begs the issue of liability. For Lockheed Martin, working with HIPAA compliant entities puts a certain onus on Lockheed Martin to follow those rules and policies. When dealing with non-covered entities, how do you determine who was in violation of items such as PII or PHI? Lockheed Martin can put all of the security management solutions in place, required of a covered entity, but in servicing a non-covered entity, how do you determine who violated a PII or PHI piece of data was shared in violation of HIPAA. Who approves access to data/information at a non-covered entity? What access authentication mechanism is employed at a non-covered entity? The issues can lead some competitive organizations to shy away from a business model with so much risk and minimal control. In terms of affecting our ability to exchange information with others, Lockheed Martin would tend to gravitate to the covered entity requirements and typically try to steer the

information sharing parameters to a place where risk is minimized and interoperability is maximized. Lockheed Martin has been extremely successful in those types of endeavors, and again, these are highlighted in the appendix.

B) Assuming you are not a covered entity, what would be the implications of complying with enforceable confidentiality, privacy, and security requirements at least equivalent to relevant HIPAA principles?

Not being a covered entity would have interesting implications in terms of complying with requirements relevant to HIPAA principles. These range in terms of cost, schedule, and performance of business activities, depending on covered entities' current level of privacy and security protections. In some cases, it may require the incorporation of confidentiality, privacy, and security systems or mechanisms to enforce compliance. In other extremes, entire business processes may need to be reconsidered. Thinking in isolation would no longer be an option. The burden of risk would increase on the entity, but likely decrease on the enterprise. The size, scope, and maturity of the entity would also have a direct barring on the impact of such changes.

C) Is there a minimum set of confidentiality, privacy, and security protections that you think everyone should follow, if not HIPAA, what?

A fundamental framework for HHS services is a must, built on the strengths of its confidentiality, privacy, and security protections; however, a closed model will

not yield the results that this country is looking for. The framework will have to provide for interfacing with multiple agencies and non-covered entities. There will need to be a governance process that ensures data maintains its confidentiality, privacy, and security regardless of the environment it traverses. HIPAA offers a sound minimum set of protections. Lockheed Martin has a vast amount of business with the federal government and civil agencies, which in more cases than not, have more stringent confidentiality, privacy, and security guidelines and policies with which we must comply. The thing to note here, is that the growing interdependence of data across the multitude of organizations requires that a growth strategy be employed that permits everyone to engage actively and be a part of the solution.

As the nation's number one Systems Integrator, Lockheed Martin has a tremendous amount of experience in delivering the type of complexity that the CPS workgroup is trying to tackle. Through our experience, we believe there are several tenets to be considered; initiatives of this size and complexity need to be approached from a systems engineering approach, change management is vital, standards are mandatory, a vetting and priority mechanism is a must, operational support is crucial (availability management, performance management, security management, configuration control, interoperability management, and many operational supporting processes). In supporting a variety of customer environments from one person in an office, to hundreds of thousands scattered around the globe, the imperatives listed above have varying degrees of impact. That impact is only further exacerbated by the amount of control a governing body has or exercises over the environment. And even in the event that the governing body has and exercises control, cycle-times and costs can get out of control very quickly. Successful implementations within the scope of CPS type activities typically depend on well planned elements of the entire system development life-cycle model.

Appendix A: Short Descriptions of Current and Past Lockheed Martin Activities Relevant to Confidentiality, Privacy, and Security

Canadian Forces Health Information System (CFHIS). CFHIS is the implementation of an integrated Electronic Health Record (EHR) in the Canadian Forces

Health Services Group. The Canadian Forces Health Information System (CFHIS) program is a program designed to enable up to 2,500 Canadian Forces (CF) health personnel located in over 80 clinics across Canada to share information securely and coordinate care for 85,000 regular and reserve force personnel, anytime, anywhere. CFHIS is an integrated Electronic Health Record (EHR) solution comprised of several different software applications brought together to create a single solution with appropriate network and security architecture. It supports master patient index, scheduling, laboratory, radiology, pharmacy, order entry and results reporting, medical charting, clinical decision support, occupational health and preventive medicine, epidemiology, social work, management reporting, patient registration/scheduling, clinical documentation, diagnostic imaging, and dental services. CFHIS provides the capability to manage health information effectively and efficiently in support of decision-making and enhanced operational effectiveness, thereby, improving the quality of health services.

Document Management Architecture (DMA). DMA provides Life Cycle Management and Operational Support Services to the Electronic Disability (eDib) process at the Social Security Administration. Through this contract, Lockheed Martin's DMA/eDib program is the largest imaging infrastructure in the world and the largest repository of HIPAA compliant medical records. 150 terabytes of storage; 1.8 million imaged daily & increasing. Lockheed Martin employs a number of confidentiality, privacy, and security

mechanisms to manage the stringent HIPAA requirements across a vast network, to ensure the integrity and protection of the SSA's data.

Department of Defense, Theater Medical Information Program (TMIP)

Lockheed Martin was selected in April 2004 to develop Block 2 of the DoD Theater Medical Information Program (TMIP). The TMIP Program collects the electronic medical records of deployed military service members, integrates that data into an overarching database and delivers the information to commanders and physicians. The benefit of TMIP is using automation to collect battlefield medical data, use this data as part of the life long medical record, and to perform medical surveillance. TMIP's integrated medical information systems ensure precise, interoperable support for rapid mobilization, deployment, and sustainment of all theater medical services anywhere, anytime, in support of any mission. TMIP is the medical component of the Global Combat Support System (GCSS). Through TMIP's Medical Surveillance System (MSS) and Joint Medical Workstation (JMeWS), Theater commanders gains situational awareness for critical decision-making. Commanders are able to track trends, take preventive action, and keep their forces fit through the ability to collect, analyze, and make use of collective medical information across Services throughout the theater in near real time. Commanders are able to determine the location and health status of injured war-fighters across the theater. TMIP integrates a clinical electronic medical record system called Composite Health Care System II-Theater (CHCS II-T), which provides clinical encounter functionality on a stand-alone laptop computer in a deployed theater

environment. CHCS II-T allows efficient recording of patient-provider interaction. Capabilities include problem lists, medication lists, allergies, immunizations, reminders, readiness reports, screening, vital signs, documenting of medical encounters, templates, and disposition. All data captured are saved in the encounter note, stored in the data repository, and are available for reporting. CHCS II-T provides individual and aggregate information on health status and population health issues.

Department of Defense, Composite Health Care System II: Requirements development, system testing, cost and benefits analysis, evaluation of results.

This clinical healthcare system has provided essential services in the development of requirements and selection of Commercial off-the-shelf products, in system testing and evaluation, and in life-cycle cost and benefits analysis. Teams of clinical experts provide functional knowledge in the test environment and in the field. Cross-functional teams provide expertise including surveys of practitioners, and measurement of healthcare processes and outcomes. Under this contract Lockheed Martin provides extensive services in projecting and reviewing the impact and importance of Electronic Health Records in the clinical and business operations of the DoD enterprise.

Department of Health and Human Services, Centers for Medicare and Medicaid Services, Consolidated Information Technology Infrastructure Contract

Under the Consolidated Information Technology Infrastructure Contract, Lockheed Martin manages mainframe, server and desktop computers, as well as the centers' voice communications infrastructure and help desk services. Lockheed Martin also handles

security and privacy services, database management, webcasting, Web hosting, and disaster recovery planning and operations for CMS under this contract. These security services manage the authentication, identity and access control systems, provisioning, role-based access, and computer security features of the entire Centers for Medicare and Medicaid infrastructure and systems.

Department of Health and Human Services, Centers for Disease Control and Prevention, CDC-Wide Information Technology Services Contract

Under this Indefinite Delivery, Indefinite Quantity vehicle, Lockheed Martin offers the CDC IT research, planning, consulting, evaluation and testing; business process re-engineering and process modeling; information systems life-cycle management; systems engineering; computer facility operations (data center, call center); technical writing and editing; QA/QC and other related services; web development and management; help desk; network operations; statistical analysis; data warehousing, data mining; GIS data entry; information security, disaster recovery; public health-related skills and services.

Department of Veterans Affairs, Veterans Health Administration, Federal Healthcare Information Exchange: architecture, design and management support.

Lockheed Martin works with both the DoD and VA in designing this critical healthcare data interchange project, to share and exchange data across the two healthcare networks, and their decentralized and disparate data systems. Services include unique identity authentication for records management, allowing the linkage of medical records across the two healthcare networks. Lockheed Martin has designed the identity management

and access control features of the system, as well as the security to prevent and/or detect breaches of security. The architecture and design includes the establishment of standards and control gates, to ensure the adherence to change and configuration management. Lockheed Martin has also developed business architecture crosswalks, organizational frameworks, and program management support to this effort.

Department of Veterans Affairs, Veterans Health Administration, One VA and MyHealth*e*Vet portal design and development.

For the VA, Lockheed Martin designed and implemented the "One VA" web portal, and the prototype for the personal healthcare portal MyHealth*e*Vet. This portal provides a web-based, single source for all relevant individual healthcare information, including upcoming and past appointments, relevant healthcare data, and access to the healthcare record itself. This effort required Lockheed Martin to integrate legacy system requirements into a web-based "front-end", addressing security and privacy concerns as they relate to authentication and access control.

Department of Defense, Defense Messaging System

Lockheed Martin is the integration contractor for the DMS. The Defense Message System (DMS) is the messaging component of the Defense Information Infrastructure (DII). The DII provides an integrated, seamless, global information common operating environment for the United States Department of Defense (DoD) for training, peacetime operations, and both tactical and mobile crisis situations. DMS is the hardware, software,

procedures, personnel, and facilities required for electronic delivery of messages among organizations and individuals in the Department of Defense. It also includes interfaces to tactical, afloat, and Allied systems. The DMS reliably handles information of all classification levels (unclassified to TOP SECRET), compartments, and handling instructions. In addition to maintaining high reliability and availability, the DMS interoperates with current message systems as it evolves from the current configuration to full implementation. The DMS is a vehicle for planned growth and technology enhancement that does not exist today. It is based upon the principles of standardization and interoperability, while preserving adaptability to implement Service and agency unique functions. DMS is standards-based and adheres to X.400 and X.500 international standards with approved extensions to meet military messaging requirements. These military messaging requirements have been accepted and approved by the U.S. allies and are formally approved in Allied Communications Publication 123 (ACP 123). DMS provides a uniform, seamless messaging system with full interoperability among the messaging assets of all DoD parties.